

Method for authentication by an external medium of a portable object such as a memory card coupled to this medium

Patent number: JP8027822B

Publication date: 1996-03-21

Inventor: HAZARD MICHEL (FR)

Applicant: BULL CP8 (FR)

Classification:

- international: G07F7/10; H04L9/32; G07F7/10; H04L9/32; (IPC1-7): G06K17/00; G06F19/00

- european: G07F7/10D4E2; G07F7/10E; H04L9/32

Application number: JP19870503572 19870615

Priority number(s): WO1987FR00221 19870615; FR19860008654 19860616

Also published as:

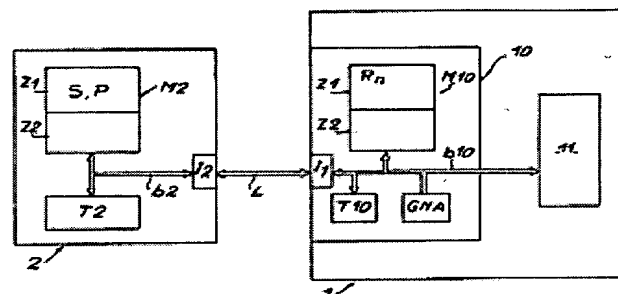
EP0250309 (A1)
WO8707743 (A1)
US5153581 (A1)
FR2600189 (A1)
EP0250309 (B1)

Report a data error here

Abstract not available for JP8027822B

Abstract of corresponding document: **US5153581**

PCT No. PCT/FR87/00221 Sec. 371 Date Feb. 12, 1988 Sec. 102(e) Date Feb. 12, 1988 PCT Filed Jun. 15, 1987 PCT Pub. No. WO87/07743 PCT Pub. Date Dec. 17, 1987. A method for authentication by an external medium of a portable object such as a standardized credit card coupled to this medium. The portable object (2) calculates a result (R) which is at least a function of a secret key (S) and of a variable datum (E). This result (R) is sampled by the external medium (1), which compares it with a reference result (RO). This result (RO) is changed in a random manner, by being replaced by a new result (RO) calculated by a portable object (2) which has been authenticated based on the preceding reference result.



Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11) 特許出願公告番号

特公平8-27822

(24) (44) 公告日 平成 8 年 (1996) 3 月 21 日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 K 17/00	T			
G 0 6 F 19/00			G 0 6 F 15/ 30	3 5 0 A

発明の数 1 (全 5 頁)

(21) 出願番号 特願昭62-503572

(86) (22) 出願日 昭和62年(1987) 6 月15日

(65) 公表番号 特表平1-502218

(43) 公表日 平成 1 年 (1989) 8 月 3 日

(86) 国際出願番号 P C T / F R 8 7 / 0 0 2 2 1

(87) 国際公開番号 W O 8 7 / 0 7 7 4 3

(87) 国際公開日 昭和62年(1987) 12 月 17 日

(31) 優先権主張番号 8 6 0 8 6 5 4

(32) 優先日 1986 年 6 月 16 日

(33) 優先権主張国 フランス (F R)

審判番号 平5-20221

(71) 出願人 999999999

ビュル セーペー 8

フランス国 78430 ルーヴシェンヌ、ベ
ペ45, ルート・ドゥ・ヴェルサイユ 68

(72) 発明者 アザール ミシェル

フランス国 78124 マレイユ/モルドゥ
ル リュ デ アリア 27

(74) 代理人 弁理士 湯浅 恭三 (外 5 名)

審判の合議体

審判長 菅野 嘉昭

審判官 内藤 二郎

審判官 赤穂 隆雄

最終頁に続く

(54) 【発明の名称】 外部装置により携帯可能な物体の正当性を証明する方法

1

【特許請求の範囲】

【請求項 1】外部装置 (1) によりこの外部装置に接続された携帯可能物体 (2) の正当性を証明するために、少なくともこの携帯可能物体 (2) のメモリ (M2) に前もって記憶された秘密キー (S) と上記外部装置 (1) から供給された変更可能な外部データ (E) との関数である結果 (R) を上記携帯可能物体 (2) の処理回路 (T2) に計算させる形式の証明方法であって、上記外部装置 (1) に以前に接続された携帯可能物体 (2) により同一の上記変更可能な外部データ (E) から計算された少なくとも 1 つの以前の結果 (Ra) と上記結果 (R) とを比較することを特徴とする、外部装置により携帯可能な物体の正当性を証明する方法。

【請求項 2】上記の変更可能なデータ (E) をもとにして参照用結果 (R0) を計算し、この参照用結果 (R0) を

2

上記外部装置 (1) のメモリ (M10) に記憶させ、上記携帯可能物体 (2) により計算された各結果 (R) が、この参照用結果 (R0) と必ず等しいことを特徴とする請求項 1 に記載の、外部装置により携帯可能な物体の正当性を証明する方法。

【請求項 3】許可された人が所持する参照用携帯可能物体 (2a) を用いて上記参照用結果 (R0) を計算させることを特徴とする請求項 2 に記載の、外部装置により携帯可能な物体の正当性を証明する方法。

【請求項 4】携帯可能物体を n 回接続した後に上記の変更可能なデータ (E) を変更し、n 自体も変更可能であることを特徴とする請求項 1 または 2 に記載の、外部装置により携帯可能な物体の正当性を証明する方法。

【請求項 5】上記外部装置から供給された新しい変更可能なデータ (E) をもとにして、以前の参照用結果に基

づいて正当であると判定されたばかりの携帯可能物体(2)を用いて、新しい参照用結果(R0)を計算させることを特徴とする請求項4に記載の、外部装置により携帯可能な物体の正当性を証明する方法。

【請求項6】上記外部装置(1)のランダム数発生器(GNA)から上記の変更可能なデータ(E)を得ることを特徴とする請求項1~5のいずれかに記載の、外部装置により携帯可能な物体の正当性を証明する方法。

【発明の詳細な説明】

本発明は、外部装置により、携帯可能な物体、例えばこの外部装置に接続されたメモカードの正当性を証明する方法に関するものである。

特に、本発明は、外部媒体がカードを介してシステムに制御命令を供給するとシステムにアクセスする許可を与える機能を有するが、所定のカードだけがこの外部媒体と連動できるようにオーソライズされているため、この外部装置に接続されたカードが制御命令の供給またはアクセス許可の権利が本来あるかどうかを、この外部装置が前もってはっきりと確認する必要がある場合に応用される。

一般に、カードなどの携帯可能物体を利用する場合には、たいいてい用途ごとに少なくとも1つの特定の秘密キーが利用される。このキーは、所定の用途にアクセス可能な全カードに前もって記憶されるとともに、この用途において制御命令を供給する、またはアクセス許可を与えるためにこのカードに接続される可能性のある全装置にも記憶される。秘密キーは、カードを発行しており、かつ、このカードと連動する装置を管理する許可を与えられた機関のみに知らされている。どの用途でも、装置は、この装置自体が記憶している秘密キーがカードの秘密キーと確かに一致していることを、秘密キーの値を明らかにすることなく確認する必要がある。

一般に、この確認作業はカードと装置の間の情報交換による対話という形態で行われる。このことは、例えば本特許出願の出願人のフランス国特許第2469,760号に記載されている。

この特許によると、対話は以下のように行う。すなわち、ランダムな数値を外部からカードに1つ入力し、カードの処理回路で計算を実行させて、このランダムな数値と前もって記憶されている秘密キーの関数である結果を導出し、この結果をカードから出力させ、この結果を装置による計算結果である少なくとも上記のランダムな数値とこの装置に前もって記憶されている秘密キーの関数である結果と比較する。

このカード確認操作またはカードの正当性の証明操作は、上記の2つの結果が一致している場合に終了する。もちろん、秘密キーが互いに等しい場合にしかこのような一致は得られない。

不正者が不正カードを製造することが絶対にできないようにするためには、特に一般人がアクセスできる装置

の段階で、使用されるキーの秘密が保持される必要がある。一般に、キーはメモリ領域に記憶され、次いで外部からアクセスできないようにロックされる。このメモリ領域には、このメモリ領域に接続された処理回路を通して内部からしかアクセスすることができない。しかし、不正行為は可能性が低く技術的に難しいとはいえ、常に可能であることを認めなくてはならない。不正者は、例えばキーが記憶されたメモリをレーザで読出す方法などの進んだ方法で秘密キーを発見しようとする。

この課題を解決するため、本発明は、秘密キーの代わりに時間経過とともに変化する情報を装置に記憶させる一方、この装置が、連動する可能性のあるカードの正当性を証明できるようにするものである。

つまり、本発明によれば、外部装置によりこの外部装置に接続された携帯可能物体の正当性を証明するために、少なくともこの携帯可能物体のメモリに前もって記憶された秘密キーと上記外部装置から供給された変更可能データの関数である結果を上記携帯可能物体の処理回路に計算させるタイプの証明方法であって、上記結果と、上記外部装置に以前に接続された携帯可能物体により同じ上記変更可能データから計算された少なくとも1つの以前の結果とを比較することを特徴とする方法が提供される。

本発明の別の特徴によれば、使用される上記の変更可能データは、外部装置により正当性が証明されたばかりの携帯可能物体によりランダムに変更される。

本発明の重要な特徴によれば、外部装置となる装置はすべてありふれた装置であり、機密情報または秘密情報をまったく記憶していない。

上記した以外の特徴、利点および詳細は、実施例を示す添付の図面を参照して行う以下の説明により明らかになる。

第1図は、本発明の方法を実行するシステムの第1の実施例の概略図である。

第2図は、本発明の方法を実行するシステムの第2の実施例の概略図である。

第1図のシステムは、装置またはターミナル1として単純化して表した外部媒体と、携帯可能物体2とで構成されている。携帯可能物体2は、所持者が例えば別のシステム(図示せず)に対する制御命令の供給を受ける、またはアクセス許可を得ることができるように一時的に装置1に接続される。

装置1は、制御装置10と、目的とする用途に応じた装置にそれぞれ対応する回路群11とに分かれている。

制御装置10は、メモリM10と、処理回路T10と、ランダム数値発生器GNAとに分かれている。これら3つの要素は、すべて制御・データ・アドレス用バスb10を介して回路群11に接続されている。メモリM10は少なくとも2つのメモリ領域1とZ2に分けられている。メモリ領域Z1は、一旦書込まれると処理回路T10によってしかアクセ

スできないデータを記憶する。これに対してメモリ領域 Z2は、読出しのときに外部からアクセスが可能であり、読出し／書込みのときに処理回路T10によってアクセス可能なデータを記憶する。

携帯可能物体 2 は例えばメモリ M2 と処理回路 T2 を備えたメモリカード (IC カード) である。メモリ M2 はプログラム可能なメモリである。また、処理回路 T2 は例えばマイクロプロセッサである。メモリ M2 と処理回路 T2 は、制御・データ・アドレス用バス b2 を介して互いに接続されている。カードのメモリ M2 はやはり少なくとも 2 つの領域 Z1 と Z2 に分けられている。それぞれの領域へのアクセス条件は装置 1 のメモリ M10 の場合と同様である。このタイプのカードは、特に、本特許出願の出願人のフランス国特許第 2, 401, 459 号と第 2, 461, 301 号に記載されている。

カード 2 と装置 1 の接続は、装置 1 側はインターフェイス I1 により、カード 2 側はインターフェイス I2 により行われる。この 2 つのインターフェイスは、近距離または遠距離を接続線 L により相互に接続されている。このような接続装置は、特に、本特許出願の出願人のフランス国特許第 2, 483, 713 号に記載されている。

カード 2 のメモリ M2 のメモリ領域 Z1 には、このカード 2 から得られる制御命令に専用の秘密キー S が記憶されている。

本発明によれば、秘密キー S が記憶されているカード 2 と連動する装置 1 にはいかなる秘密キー S も記憶されていない。

第 1 図の実施例に従って、この場合でも、装置 1 に接続されており秘密キー S が記憶されたカード 2 の正当性をこの装置 1 が証明可能であることを説明する。

装置 1 はカード 2 にランダムな数値 E を送る。カード 2 の処理回路 T2 はメモリ領域 Z1 に前もって記憶されているプログラム P を実行する。このプログラム P は、少なくとも上記のランダムな数値 E と秘密キー S を考慮して、以下の式

$$R = f(E, S)$$

で表される結果 R を計算する。

このようにして得られた結果は次に装置 1 の制御装置 10 に送られて解析され、カード 2 の有効性が判定される。

このためには、n 枚のカード 2 が既に装置 1 に接続されたことがあると仮定する。これら n 枚のカードは n 個の計算結果 Ra を既にそれぞれ計算して制御装置 10 のメモリ領域 Z1 に次々と記憶させている。ここでさらに、これら n 個の計算結果がすべて同一のランダムな数値 E から計算されたものと仮定する。ところで、ランダムな数値 E は、発生器 GNA から出力された後に制御装置 10 のメモリ M10 のメモリ領域 Z2 に記憶されている。

カード 2 の正当性の確認は、結果 R をそれ以前の結果 Ra と比較することにより行う。実際には、4 つの場合が

考えられる。

最初の 2 つの場合には、以前の結果 Ra がすべて同じであると仮定されている。すなわち、以前の結果 Ra はすべて、同一の用途に対する同一の秘密キー S を記憶しているカードにより同一のランダムな数値 E から計算されたものである。

第 1 の場合には、結果 R はそれぞれの結果 Ra と等しい。すると制御装置 10 はカード 2 が正当なものであると判断して、装置 R を記憶させる。次にこの結果 R は古い結果 Ra となって装置 1 に回路群 11 の作動を許可する制御信号を発生させる。

第 2 の場合には、結果 R がそれぞれの結果 Ra と異なる。すると制御装置 10 はカード 2 が不正なものであると判断して回路群 11 の作動を禁止する。

第 3 の場合と第 4 の場合には、以前の結果 Ra は必ずしもすべてが互いに等しくはないと仮定されている。すなわち、以前の結果 Ra は異なった用途に対する異なった秘密キー S から計算されたものである。

上記の各場合には、各カード 2 により計算された様々な結果 R が制御装置のメモリ M10 に記憶されている。メモリを節約するためには同じ結果を重複しては記憶させないで、異なった結果が現れた最初のときにその結果 R を記憶させるとともに、カウンタを用い、新しい結果 R が既に記憶された結果と同じであるときにはそのたびごとにこのカウンタをインクリメントするのが好ましい。

利用者のカード 2 ごとにさらにモニタ操作を行うことにより、同一のカード、特に不正なカードが n 回連続して装置 1 に接続されることがあっても、この装置 1 が騙されて、カード 2 により計算されたすべて同一の以前の結果 Ra が正当で、n 枚の異なる正当なカードから得られたものであると判定することがないようにするのが好ましい。このモニタ操作は、カード所持者に固有のデータ、例えばカードのシリアル番号を装置 1 に記憶させ、同一のカードがこの装置に接続された回数をモニタすることにより行う。

このような構成にすると、参照用の結果 R がまだ外部装置 1 に記憶されていない時、あるいは記憶されている参照用結果 Ra の種類が極めて少ない場合に、携帯可能な物体 2 を最初に挿入したとき外部装置がどのように動作するかを設計する際に、次に二つの可能性が考えられる。

(a) 挿入される携帯可能な物体 2 に対応する以前の結果が記憶されていない場合、携帯可能な物体によって送られたいづれの結果も正しい、と判断するように設計する、あるいは、

(b) 以前の結果が記憶されていない場合、送られた結果はすべて誤りであり、この場合、いかなる物体の正当性も証明されない、と判断する、という以上の二つである。

いずれにしても、このままでは最初のユーザに対して

はそのカードの正当性を検証することは不可能である。

この問題は、第2図に示した第2の実施例のようにして、この装置1を管理する許可を与えられている機関が先ず参照用の結果R0を書き込むようにすることによって解決される。この図の装置1では、この装置1を管理する許可を与えられている機関が使うことのできる参照用カード2aに記憶されている特定の用途に対応する秘密キーSを用いて参照用結果R0が計算される。そしてこの参照用結果R0が、この機関が提供する特定の用途を利用するために装置1にアクセス可能な全カードに共通な同一の秘密キーSに対する最初の参照用結果として外部装置1のメモリM10のメモリ領域Z1に記憶される。

第2図の参照用カード2aは第1図のカード2と同じタイプのカードである。許可を得た人がこの参照用カード2aを装置1に接続すると、この装置1内のランダム数値発生器GNAはランダムな数値Eを出力して参照用カード2aに送る。参照用カード2aの処理回路T2は、結果Rの計算の場合と同様にして参照用結果R0を計算する。この参照用結果R0は制御装置10のメモリM10のメモリ領域Z1に記憶される。次に、カード2で計算された各結果Rがこの参照用結果R0とだけ比較される。この場合、制御装置のメモリM10に様々なカード2により計算された結果を記憶させる必要はない。

本発明の重要な特徴によると、ランダムな数値Eは安全のために変更することができる。この変更は定期的に行うのではなく、例えば装置にn枚のカードが接続された後に行う。この数nは変えることができる。ラン*

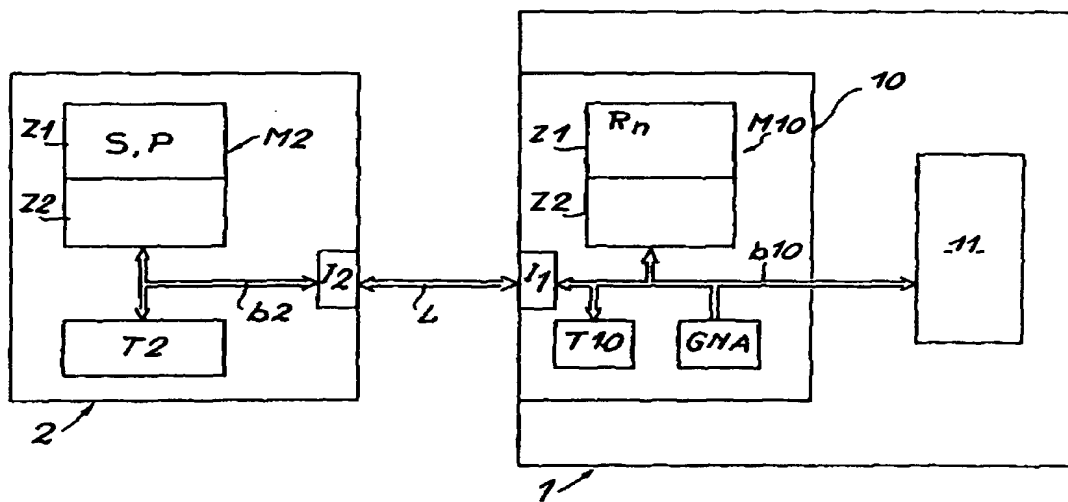
*ダムな数値Eを変更するという事は、新しい参照用結果R0を計算することを意味する。この計算を行うためには、初期化のために以前に用いた参照用カード2aを用いることができる。この解決法は十分なものではない。というのは、変更のたびごとに、この参照用カード2aの所持を許可された人が各装置1のところにしかけることを意味するからである。

本発明では、まったく簡単に、以前の参照用結果R0をもとにして正当であると判定された利用者のカード2により新しい参照用結果R0を計算する。従って、参照用カード2aを用いる必要はない。

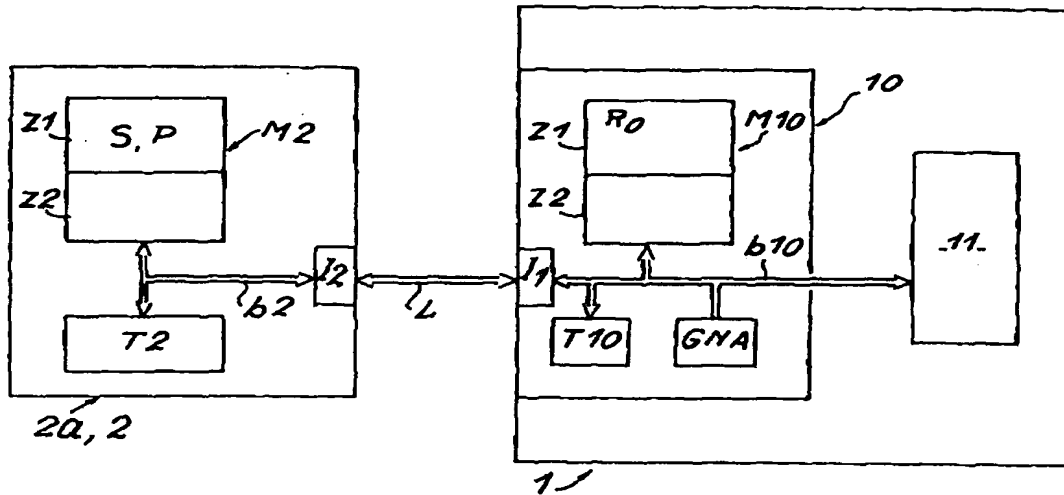
さらに詳しく説明すると、n番目のカード2 (nは変更可能) が正当であると判定されると、装置1のランダム数値発生器GNAがランダムな数値Eをカード2に出力する。するとこのカード2のマイクロプロセッサT2が新しい参照用結果R0を計算する。次に、この参照用結果R0のほか、出力されたばかりのランダムな数値Eが装置1のメモリM10に記憶される。

本発明の装置1を用いると、カード2の正当性をこれからカードに記憶された秘密キーSに基づいて確認することができる。しかも、秘密キーを知る必要がなく、再計算する必要もない。このときに確認されるのは、同一の秘密キーを有するカードのみであ。また、複数の異なる秘密キーSに対応する複数の結果を装置1から発生させ、複数種のカードの正当性を判定することが可能である。この場合、それぞれの種類のカードは装置1で確認可能な所定の秘密キーを記憶している。

【第1図】



【第2図】



フロントページの続き

- (56) 参考文献 特開 昭59-77575 (J P, A)
 特開 昭60-181891 (J P, A)
 特開 昭59-139479 (J P, A)
 米国特許3798605 (U S, A)
 米国特許4471216 (U S, A)